IPAC

tra-governmental Payment and Collection System

Please TYPE or legibly PRINT your information

User Registration Form

Check one box:

□ New Request
□ Update
□ Revoke

Section I – User Information *(all fields are required)*

Treasury UPS User ID ____________________
Name (First, Middle Initial, Last) ____________________ _____ ____________________
Master ALC ____________________
Email Address ____
Complete Work Phone

Section II – Access requested

For IPAC and TRACS, provide the ALC(s) for which access is required; provide the Payroll Office number for access to RITS. For each ALC or Payroll Office, circle the user role(s) for which access is to be granted. If applicable, more than one role may be selected per application.

ALC or PAYROLL OFFICE	MODULE	ROLE(S)					
	IPAC	IPAC Reports	IPAC User	IPAC Supervisor	IPAC Bulk File Submitter	IPAC Bulk Automation	IPAC Online 3rd Party
	TRACS	TRACS Reports					
	RITS	RITS Accountant	RITS Payroll Clerk	RITS Payroll Admin	RITS Bulk File Submitter	RITS Bulk Automation	
	IPAC	IPAC Reports	IPAC User	IPAC Supervisor	IPAC Bulk File Submitter	IPAC Bulk Automation	IPAC Online 3rd Party
	TRACS	TRACS Reports					
	RITS	RITS Accountant	RITS Payroll Clerk	RITS Payroll Admin	RITS Bulk File Submitter	RITS Bulk Automation	

____________________ Name and Title of Supervisor
____________________ Supervisor Signature
__________ Telephone #
__________ Date

FOR AA USE ONLY: (Complete this section when you have completed a review of the request)

____________________ Administrator Name
____________________ Administrator Signature
__________ Telephone #
__________ Date

User: Return completed User Registration Form and signed Rules of Behavior to your AA.
AA: Sign completed User Request Form and Fax completed form, along with the signed Rules of Behavior to the Treasury Support Center at 314-444-7346

IPAC
tra-governmental Payment and Collection System

IPAC System User Roles and Functions

IPAC

User Role	Function Performed
IPAC Reports	• View system messages • Access to the following reports: Agency Special Requirements Headquarters Transactions Headquarters Transaction Download IPAC and Zero Dollar Transactions IPAC Transaction Download Parent / Child Relationships Predecessor / Successor ALCs Sender Required Fields Treasury Reporting Requirements • Review reports / data files • Purge reports / data files
IPAC User	Same access rights as the IPAC Reports role, plus • Process payment, collection, adjustment and zero dollar transactions • Complete incomplete transactions • View status of agency special requirements request • Add/edit SGL information to transactions received / sent
IPAC Supervisor	Same access rights as the IPAC Reports role, plus • Request an update to agency billable status • View agency billable status • Request an update to agency special requirements • View status of agency special requirements request • Request establishment of a parent / child relationship • Update agency information
Bulk File Submitter	• Submit bulk IPAC transactions • Review bulk file status information (including confirmation/ rejection information) • Display messages • Review reports / data files (future release) • Purge reports / data files
IPAC Bulk Automation	• Submit bulk IPAC transactions
Online 3rd Party	• Used by only select ALCs that enables an ALC to submit transactions on behalf of other sender and receiver ALCs. • Access to the following: Agency Special Requirements IPAC transactions IPAC transaction download Predecessor / Successor ALCs Third Party Submitter Treasury Reporting Requirements

User: Return completed User Registration Form and signed Rules of Behavior to your AA.
AA: Sign completed User Request Form and Fax completed form, along with the signed Rules of Behavior
to the Treasury Support Center at 314-444-7346

TRACS

User Role	Function Performed
TRACS Reports	• Display messages • Access to TRACS Reports • Review reports / data files • Purge reports / data files

RITS

User Role	Function Performed
RITS Accountant	• Display Messages • View list of all health benefit codes • Access to the following reports: Computer generated 2812 or 2812A Enrollment codes Holiday schedule • Review reports / data files • Purge reports / data files
RITS Payroll Clerk	Same access rights as the RITS Accountant role, plus • Manage 2812
RITS Payroll Admin	Same access rights as the RITS Accountant role, plus • Manage 2812 • Maintain payroll office / pay cycle
Bulk File Submitter	• Submit bulk 2812s • View system messages • Access to confirmation / rejection report • Review reports / data files • Purge reports / data files
RITS Bulk Automation	• Submit bulk 2812s

User: Return completed User Registration Form and signed Rules of Behavior to your AA.
AA: Sign completed User Request Form and Fax completed form, along with the signed Rules of Behavior to the Treasury Support Center at 314-444-7346

Rules of Behavior

Terms of Use

Please read and accept the Terms of Use in order to complete your access request.

GENERAL

- **Exercise only those IPAC System capabilities assigned to you by your Organization or Unit IPAC Security Administrator.**

  Each User registered to access the IPAC system will have a unique User ID. One of those specific roles may be assigned to each user. The level of authority available to a user in a role will determine the level of user authentication required to allow execution of the role. Both User ID and authentication information are the property of the IPAC System and the user. Transfer of User ID and authentication to another can result in loss of IPAC System access privileges. Attempting to exercise roles other than those assigned by any means can result in loss of IPAC System access. Only one Master Administrator will give each Agency Administrator access authority. Only one Agency Administrator will give each IPAC user access authority. Each Agency Administrator will have a backup.

- **Provide appropriate controls over sensitive information available from IPAC.**

  Information available from the IPAC System may be considered sensitive (Privacy Act), sensitive (Business), restricted or classified.

  Sensitive (Privacy Act) information is any information in IPAC that relates to an individual by name, social security number or traceable characteristic (User ID, telephone number, etc.) to a financial transaction affecting that individual. Sensitive (Privacy Act) information must be controlled as defined in The Privacy Act of 1974, 5 USC & 552A – as amended.

  Sensitive (Business) information is any information in IPAC except that information appearing specifically on financial reports released to the Public by appropriate authority and then only in the context of the public report. Sensitive (Business) information can be released only to those individuals having a business need to see or use it.

  The IPAC System will allow only those users with appropriate formal clearance to access the restricted information. If restricted information is available to you and you have neither appropriate clearance and need to know, it is your responsibility to report the incident and associated circumstance to your Agency Administrator or your Master Administrator.

- **Understand and comply with applicable policies and procedures related to your access to, and use of, IPAC resources.**

  Your organization has its own policies and procedures related to access and use of information available through your organization Intranet or Internet. Your organization may have policies and procedures related to distribution of financial information within the organization and to external organizations. Your internal policies and procedures will be available through your Master Administrator or your Agency Administrator.

User: Return completed User Registration Form and signed Rules of Behavior to your AA.
AA: Sign completed User Request Form and Fax completed form, along with the signed Rules of Behavior
to the Treasury Support Center at 314-444-7346

- **Identify potential risks to IPAC System and information integrity, timeliness or sensitivity to the appropriate organization authority.**

  Since the financial management data and information in the IPAC System is the U.S. Department of the Treasury's picture related to user agency financial status, it is critical that all who use the system and data participate in identifying conditions or actions which will impede the integrity, timeliness or sensitivity of the IPAC System or data. Risks internal to your organization must be reported through your internal security point of contact. Apparent risks to the IPAC System itself must be identified through your Master Administrator, Agency Administrator, or the FMS Administrator.

- **Identify inhibitors to effective performance of your IPAC System related responsibilities to the appropriate organization authority**

  Inhibitors to your effective performance of the IPAC System related tasks pertaining to intra-governmental transfers have direct impact on the integrity of IPAC information available for decision making and reporting. Inhibitors fit into two categories – IPAC System oriented and organization infrastructure or system oriented. IPAC System inhibitors to your performance include such things as time to download information, download media, content of records or screens, availability of detail to support research, and the like. To report your IPAC System inhibitors contact the Treasury Support Center at 866-809-5218.

SPECIFIC

USERS must ensure that the information technology (IT) resources with which they have been entrusted are used properly, as directed by FMS policies and standards, taking care that the laws, regulations, and policies governing the use of such resources are followed and that the value of all information assets are preserved. Each user is responsible for all activities associated with their assigned User ID.

USERS must be knowledgeable about FMS IT policies and standards. As systems change, users are required to seek additional information in order to ensure current policies and procedures are followed.

USERS must take positive steps to protect FMS data from unauthorized users.

USERS must not attempt to circumvent any FMS IT security control mechanisms.

USERS must follow proper login/logoff procedures.

USERS must complete IR security awareness, training and education as required by their agency's policies and procedures.

USERS must not read, alter, insert, copy, or delete any FMS data except in accordance with assigned job responsibilities. Ability to access data does not equate to authority to manipulate data. In particular:

USERS must not browse or search FMS data except in the performance of authorized duties.

USERS must not reveal information produced by the FMS application except as required by job function and within established procedures.

USERS must protect FMS communications/connectivity integrity.

USERS must comply with and provide assistance with IT audits and reviews as appropriate

USERS must report any known or suspected breaches of IT security to security administrators immediately after discovery of the occurrence.

USERS must retrieve all hard copy printouts in a timely manner.

USERS must ensure that unauthorized individuals cannot view screen contents.

USERS must protect User IDs and passwords from improper disclosure. Passwords provide access to FMS data and resources.

USERS are responsible for any access made under his/her User ID and password.

USERS do not reveal Passwords under any circumstances. Password disclosure is considered a security violation and is to be reported as such. If Password disclosure is necessary for problem resolution, immediately select a new password once the problem has been resolved.

Do not program login IDs or Passwords into automatic script routines or programs.
Do not share Passwords with anyone else or use another person's Password.
Do not write Passwords down.
Change Passwords in accordance with the system/application requirements.
Choose hard to guess Passwords, in accordance with the system/application requirements.

ACCEPTANCE

I have read the Financial Management (FMS) Information technology Terms of Use and fully understand the security requirements of the information systems, modules and data. I further understand that violation of these rules may be grounds for administrative and/or disciplinary action by agency officials and may result in actions up to and including termination or prosecution under Federal law.

[ ] Accept **[ ] Do Not Accept**

Print Name: ________________________________ Date: ______________________

Signature: ____

User: Return completed User Registration Form and signed Rules of Behavior to your AA.
AA: Sign completed User Request Form and Fax completed form, along with the signed Rules of Behavior to the Treasury Support Center at 314-444-7346